Advanced Network Forensics

Outline

- Flow based Vs Packet based
  - Argus
  - Tcpdump
  - Snort
  - Chopshop
  - Volatililty
- Demo
  - Tracking C&C
  - System Investigation

Flow based - Netflow

- Flow based Network Security Analysis centers around the concept of a network flow/traffic instead of each packet.
- A flow record is a summarized indicator that a certain network flow took place and that two hosts have communicated with each other at some point in the past.

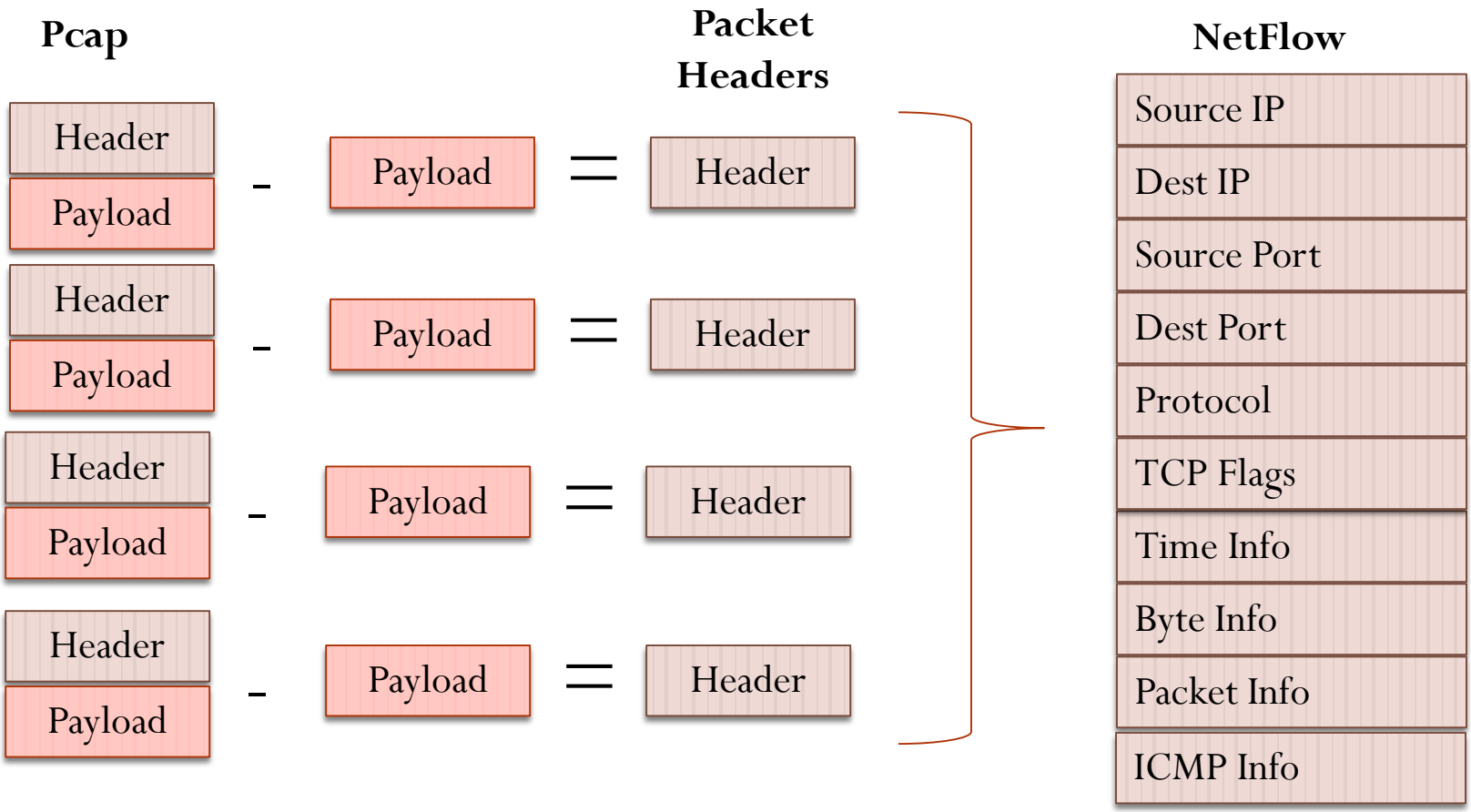
What netflow data is not

- Replacement for full packet capture
- If you care about the content of the message continue to use full packet capture
- Netflow is like a phone bill
  - You know who called who, but not what was said

Packet Based

- Packet-based network security analysis, unlike flow-based solutions, does not rely on third-party components to generate meta or summary information of the network traffic.
- Instead, all analysis is entirely based on actually observed raw packets, as they traverse the network links. It focuses on each packet or a group of packets.

Netflow data, the “diet” pcap



Argus

- the network Audit Record Generation and Utilization System
- The Argus Project is focused on developing all aspects of large scale network activity audit.
- Argus, itself, is next-generation network flow technology, going from packets on the wire to advanced network flow data, to network forensics data; all in support of Network Operations, Performance and Security Management.

Argus

- Converting Pcap to netflow
  - argus –r packet.pcap –w packet.argus
- Reading a netflow file
  - ra –r netflowfile

Tcpdump

- a powerful command-line packet analyzer; and *libpcap*, a portable C/C++ library for network traffic capture.

Tcpdump

- Basic communication (very verbose)
  - # tcpdump -nnvvS
- Capture all Port 80 Traffic to a File
  - # tcpdump -s 1514 port 80 -w capture_file
- Read Captured Traffic back into tcpdump
  - # tcpdump -r capture_file

Snort

- A free lightweight network intrusion detection system for UNIX and Windows.
- Example rule for icmp:
  - alert icmp any any -> any any (msg:"ICMP Packet"; sid:477; rev:3;)

Chopshop

- http://www.github.com/MITRECND/chopshop
- MITRE-developed packet framework
  - Based on libnids
  - TCP reassembly
  - Handles boilerplate code
  - Python
  - Great for rapid prototyping

Chopshop

- Framework provides a standard API
- Framework does not analyze packets
- Modules provide all the brains
- Invoke with a list of PCAP files and modules

Chopshop

$ chopshop -f http.pcap “payloads ”

- Run payloads module on http.pcap

$ find pcaps -type f |

> chopshop “payloads ”

- Run payloads on all files in pcaps directory

Volatililty

- An advanced memory forensics framework
- Volatility supports investigations of the memory images
- Example:
  - $ python vol.py --info Volatility Foundation Volatility Framework 2.4

Exercises

- What is the C2?
- What tools were placed on the machine?
- What type of backdoor?
- What was stolen?
- What process id was the backdoor running in?
- What was the name of the dropper?